CLAIMS

What is claimed is:

1. A method of establishing a secure wireless communications channel between an access point and a station, the channel being encrypted with a channel key, the method comprising:

sending, by the station to the access point, a request for a security preference for the access point;

sending, by the access point to the station, the security preference in response to the request when the access point can support the channel;

generating, by the station, authentication information using a first key when the security preference is shared key;

sending, by the station to the access point, the authentication information;

validating, by the access point, the station using the authentication information;

encrypting, by the access point, the channel key using a second key when the station is validated;

sending, by the access point to the station, the encrypted channel key;

decrypting, by the station, the channel key in response to receiving the encrypted channel key; and

sending, by the station to the access point, data encrypted with the channel key to establish the channel.

2. The method of claim 1, wherein the first and second keys are a self-distributed key.

3. The method of claim 2, further comprising:

generating, by the access point, the self-distributed key using a security algorithm when the security preference is shared key;

generating, by the station and sending to the access point, a first value using the security algorithm in response to receiving the security preference of shared key;

generating, by the access point, and sending to the station, a second value using the security algorithm and the first value in response to receiving the first value; and

calculating, by the station, the self-distributed key using the security algorithm and the second value in response to receiving the second value.

4. The method of claim 3, wherein the security algorithm is $g^n \bmod p$ and further comprising:

obtaining, by the access point, integers x, g and p to generate the self-distributed key $k = g^x \bmod p$;

obtaining, by the station, the integers g and p, and an integer y to generate the first value $Y = g^y \bmod p$;

generating, by the access point, the second value $X = Y^x \bmod p$; and

setting, by the station, z equal to y^{-1} to calculate the self-distributed key $k = X^z \bmod p$.

5. The method of claim 4 wherein obtaining, by the station, the integers g and p comprises:

sending, by the access point to the station, the integers for g and p.

6. The method of claim 5, wherein the integers for g and p are sent to the station when the security preferences are sent by the access point.

7. The method of claim 5, wherein the integers for g and p are sent to the station when a user name and password for the station are registered with the access point.

8. The method of claim 4 further comprising:

publishing, by the access point, the integers g and p for a set of stations.

9. The method of claim 2 further comprising:

encrypting, by the station, a name and password with the first key to generate the authentication information; and

decrypting, by the access point, the name and password to validate the station.

10. The method of claim 2 further comprising:

sending, by the access point to the station, a challenge;

encrypting, by the station, the challenge with the first key to generate the authentication information;

encrypting, by the access point, the challenge with the first key; and

comparing, by the access point, the authentication information with the challenge encrypted by the access point with the first key to validate the station.

11. The method of claim 1, wherein the first key is a public key of a public-private key pair for the access point, and the second key is a public key of a public-private key pair for the station.

12. The method of claim 11 further comprising:

sending, by the access point to the station, the first key; and.

sending, by the station to the access point, the second key.

13. The method of claim 12, wherein the second key is sent to the access point when the request for the security preference is sent by the station.

14. The method of claim 12, wherein the first key is sent to the station when the security preference is sent by the access point.

15. The method of claim 1, wherein establishing the channel creates a standard wired equivalent privacy (WEP) network, and the station and the access point exchange messages conforming to a format required by the standard that defines a WEP network to establish the WEP network.

16. A method for connecting a station to a secure wireless network comprising:

sending a request for a security preference to an access point for the secure wireless network;

generating authentication information for the station when the station receives a security preference specifying shared key from the access point;

sending the authentication information to the access point;

decrypting a channel key in response to receiving an encrypted channel key from the access point; and

sending data encrypted with the channel key to the access point.

17. The method of claim 16 further comprising:

generating a first value using a security algorithm in response to receiving the security preference specifying shared key from the access point;

calculating a self-distributed key using the security algorithm and a second value in response to receiving the second value from the access point; and

using the self-distributed key to generate the authentication information and to decrypt the encrypted channel key.

18. The method of claim 17, wherein the security algorithm is formulated as $g^n \bmod p$ and further comprising:

obtaining integers for y, g and p to generate the first value $Y = g^y \bmod p$; and

setting z equal to y^{-1} to calculate the self-distributed key $k = X^z \bmod p$.

19. The method of claim 16 further comprising:

using a first key to generate the authentication information; and

using a second key to decrypt the encrypted channel key.

20. The method of claim 19, wherein the first key is a public key of a public-private key pair for the access point, and the second key is a private key of a public-private key pair for the station.

21. A method of securing a wireless network at an access point comprising:

sending a security preference in response to a request from a station;

validating the station in response to receiving authentication information from the station;

encrypting a channel key when the station is validated;

sending the encrypted channel key to the station; and

sending data encrypted with the channel key to the station.

22. The method of claim 21 further comprising:

generating a self-distributed key using a security algorithm when the security preference is shared key;

generating a second value using the security algorithm and a first value in response to receiving the first value from the station; and

sending the second value to the station.

23. The method of claim 22, wherein the security algorithm is formulated as $g^n \bmod p$ and further comprising:

obtaining integers x, g and p to generate the self-distributed key $k = g^x \bmod p$; and

generating the second value $X = Y^x \bmod p$.

24. The method of claim 21 further comprising:

using a first key to evaluate the authentication information; and

using a second key to encrypt the encrypted channel key.

25. The method of claim 24, wherein the first key is a private key of a public-private key pair for the access point, and the second key is a public key of a public-private key pair for the station.

26. A computer-readable medium having stored thereon executable instructions to cause a processor to perform a station method to connect to a secure wireless network, the instructions comprising:

sending a request for a security preference to an access point for the secure wireless network;

generating authentication information for the station when the station receives a security preference specifying shared key from the access point;

sending the authentication information to the access point;

decrypting a channel key in response to receiving an encrypted channel key from the access point; and

sending data encrypted with the channel key to the access point.

27. The computer-readable medium of claim 26 having further instructions comprising:

generating a first value using a security algorithm in response to receiving the security preference specifying shared key from the access point;

calculating a self-distributed key using the security algorithm and a second value in response to receiving the second value from the access point; and

using the self-distributed key to generate the authentication information and to decrypt the encrypted channel key.

28. The computer-readable medium of claim 27, wherein the security algorithm is formulated as $g^n \ mod \ p$ and having further instructions comprising:

obtaining integers y, g and p to generate the first value $Y = g^y \ mod \ p$; and

setting z equal to y^{-1} to calculate the self-distributed key $k = X^z \ mod \ p$.

29. The computer-readable medium of claim 26 having further instructions comprising:

using a first key to generate the authentication information; and

using a second key to decrypt the encrypted channel key.

30. The computer-readable medium of claim 29, wherein the first key is a public key of a public-private key pair for the access point, and the second key is a private key of a public-private key pair for the station.

31. A computer-readable medium having stored thereon executable instruction to cause a processor to perform an access point method to secure a wireless network, the instructions comprising:

sending a security preference in response to a request from a station;

validating the station in response to receiving authentication information from the station;

encrypting a channel key when the station is validated;

sending the encrypted channel key to the station; and

sending data encrypted with the channel key to the station.

32. The computer-readable medium of claim 31 having further instructions comprising:

generating a self-distributed key using a security algorithm when the security preference is shared key;

generating a second value using the security algorithm and a first value in response to receiving the first value from the station; and

sending the second value to the station.

33. The computer-readable medium of claim 32, wherein the security algorithm is formulated as $g^n \bmod p$ and having further instructions comprising:

obtaining integers x, g and p to generate the self-distributed key $k = g^x \bmod p$; and

generating the second value $X = Y^x \bmod p$.

34. The computer-readable medium of claim 31 having further instructions comprising:

using a first key to evaluate the authentication information; and

using a second key to encrypt the encrypted channel key.

35. The computer-readable medium of claim 34, wherein the first key is a private key of a public-private key pair for the access point, and the second key is a public key of a public-private key pair for the station.

36. A secure wireless network comprising:

an access point operable for receiving a connection request from a station through a setup connection, for validating authentication information sent by the station, and for connecting the station to the network through a channel secured with a shared channel key; and

a station operable for sending the connection request to the access point, and for generating the authentication information to send to the access point.

37. The secure wireless network of claim 36, wherein the access point is further operable for sending a security preference specifying shared key to the station upon receiving the connection request, and the station is operable for sending the authentication information to the station upon receiving a security preference specifying shared key.

38. The secure wireless network of claim 37, wherein the access point is further operable for encrypting the shared channel key using a self-distributed key for sending to the station and the station is further operable for decrypting the shared channel key upon receipt.

39. The secure wireless network of claim 38, wherein the station and the access point are further operable for calculating the self-distributed key by exchanging messages in accordance with the Hughes transmission protocol

40. The secure wireless network of claim 36, wherein the station is further operable for using a first key to generate the authentication information and for using a second key to decrypt an encrypted shared channel key received from the access point, and the access point is further operable for using a third key to evaluate the authentication information and for using a fourth key to encrypt the shared channel key for sending to the station.

41. The secure wireless network of claim 40, wherein the first and third keys are public and private keys, respectively, for the access point, and the second and fourth keys are private and public keys, respectively, for the station.

42. A computer-readable medium having stored thereon a message data structure for a secure wireless network comprising:

a station address field containing data representing an identifier for a station that exchanges messages with an access point on the secure wireless network;

a transaction sequence number field containing data representing a sequence number for a message exchanged between the station identified by the station address field and the access point;

an authentication algorithm field containing data representing an identifier for a protocol used by the access point to validate the station identified by the station address field based on a name and password for the station; and

a dependent information field containing data required to connect the station identified by the station address field to the secure wireless network.

43. The computer-readable medium of claim 42, wherein the data in the dependent information field represents key information for encrypting the name and password for the station identified by the station address field.

44. The computer-readable medium of claim 42, wherein the data in the dependent information field represents an encrypted name and password for the station identified by the station address field.

45. The computer-readable medium of claim 42, wherein the data in the dependent information field represents an encrypted channel key used to connect the station identified by the station address field to the secure wireless network.